PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-051818
(43)Date of publication of application : 21.02.2003

(51)Int.Cl. H04L 9/08
H04L 9/32
H04L 12/66
H04Q 7/38

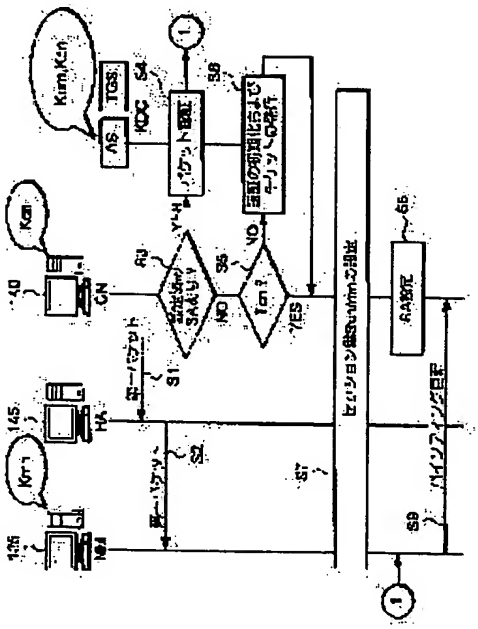
(21)Application number : 2002-102816
(22)Date of filing : 04.04.2002

(71)Applicant : DOCOMO COMMUNICATIONS LABORATORIES USA INC
(72)Inventor : YOKOTE AKI

(30)Priority
Priority number : 2001 827632 Priority date : 06.04.2001 Priority country : US

(54) METHOD FOR IMPLEMENTING IP SECURITY IN MOBILE IP NETWORKS

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a method of implementing IPsec (Internet Protocol Security) in third generation and beyond wireless, mobile access, Internet protocol- based digital networks supporting Mobile IP.
SOLUTION: A sending node initiates establishment of a security association for a receiving node, rather than waiting for the receiving node to initiate security association establishment after receiving a packet from the sending node. Thus, the disclosed method greatly reduces the packet delay introduced by required authentication and security association establishment processes. The IPsec may use the Kerberos key exchange method. The Kerberos key exchange method, since it requires less computational overhead, is a suitable IPsec method for mobile IP networks where PDAs and cellular phones are primary network access devices and packet delay associated with authentication and security processes are further reduced.



LEGAL STATUS

[Date of request for examination] 04.04.2002
[Date of sending the examiner's decision of rejection] 04.10.2005
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2003－51818
（P2003－51818A）
(43)公開日　平成15年２月21日(2003.2.21)

(51)Int.Cl.'		識別記号	FI		テーマコード'(参考)
H04L	9/08		H04L	12/66	B　5J104
	9/32			9/00	601C　5K030
	12/66		H04B	7/26	109S　5K067
H04Q	7/38		H04L	9/00	601E
					675Z

審査請求　有　請求項の数21　ＯＬ　（全 17 頁）

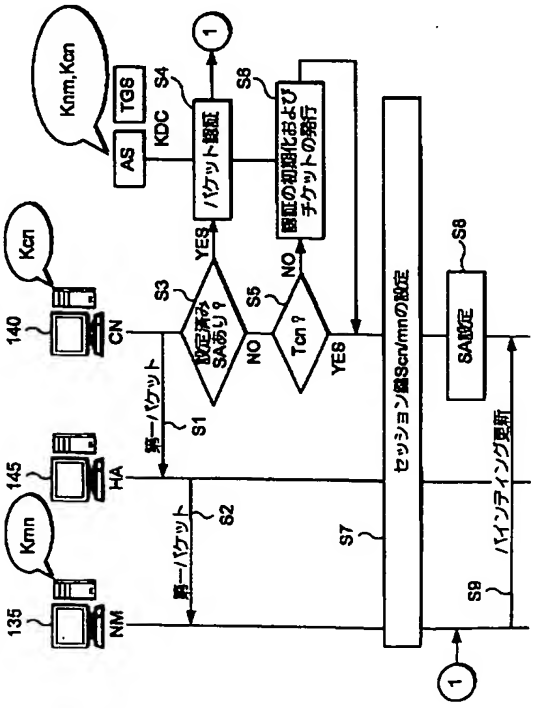
(21)出願番号　特願2002－102816(P2002－102816)
(22)出願日　平成14年４月４日(2002.4.4)
(31)優先権主張番号　０９／８２７６３２
(32)優先日　平成13年４月６日(2001.4.6)
(33)優先権主張国　米国（ＵＳ）

(71)出願人　301077091
ドコモ　コミュニケーションズ　ラボラトリーズ　ユー・エス・エー　インコーポレーティッド
アメリカ合衆国，カリフォルニア州　95110，サンノゼ，スイート300，メトロドライブ　181
(74)代理人　100098084
弁理士　川▲崎▼　研二　（外１名）

最終頁に続く

(54)【発明の名称】　モバイルＩＰネットワークにおけるＩＰセキュリティ実行方法

(57)【要約】
【課題】　モバイルＩＰをサポートする第三世代若しくはこれを超える世代の無線移動アクセスインターネットプロトコルを用いたデジタルネットワークにおいて、ＩＰｓｅｃを実行する方法を提供する。
【解決手段】　送信ノードは、受信ノードが当該送信ノードからパケットを受信した後にセキュリティアソシエーションの設定を初期化するのを待つのではなく、受信ノードに対応したセキュリティアソシエーションの設定を初期化する。これによって、必要な認証およびセキュリティアソシエーションの設定に起因するパケット遅延は劇的に減少する。ＩＰｓｅｃはケルベロス鍵交換法を用いても良い。ケルベロス鍵交換法は計算量が少なくて済むので、主にＰＤＡや携帯電話機等が接続するモバイルＩＰネットワークにおいて適しており、認証およびセキュリティ設定処理において発生してしまうパケット遅延はさらに減少する。



1

【特許請求の範囲】

【請求項１】　移動ＩＰネットワークにおいてインターネットプロトコルセキュリティを実行する方法であって、

第一ノードからの第二ノードに対する通信を初期化する過程と、

前記第一ノードが、前記第二ノードにおいてセキュリティアソシエーションが設定されているかどうかを判断する過程と、

前記第一ノードが、前記第二ノードにおいてセキュリティアソシエーションが設定されていない場合は、前記第二ノードと行う通信を保護するためのセキュリティアソシエーションの設定を初期化する過程とを有することを特徴とするインターネットプロトコルセキュリティ実行方法。

【請求項２】　前記第二ノードは、自身のホームリンクの外部に位置する移動ノードであることを特徴とする請求項１に記載のインターネットプロトコルセキュリティ実行方法。

【請求項３】　前記第一ノードは、前記第二ノードのホームエージェントを介して前記第二ノードへ制御パケットを送信することによって前記第二ノードとの通信を初期化し、前記第二ノードはそれに対する応答として、バインディング更新を前記第一ノードへ送信することを特徴とする請求項２に記載のインターネットプロトコルセキュリティ実行方法。

【請求項４】　前記設定されるセキュリティアソシエーションには、ケルベロス鍵交換法が用いられることを特徴とする請求項１記載のインターネットプロトコルセキュリティ実行方法。

【請求項５】　前記第一ノードおよび前記第二ノードの少なくとも１つは、第二層で設定される秘密鍵を第三層での認証に用いることを特徴とする請求項４記載のインターネットプロトコルセキュリティ実行方法。

【請求項６】　前記ネットワークはセキュリティアソシエーション管理装置を有し、前記セキュリティアソシエーションは前記セキュリティアソシエーション管理装置によって設定されることを特徴とする請求項１記載のインターネットプロトコルセキュリティ実行方法。

【請求項７】　前記第一ノードおよび前記第二ノードは加入者識別モジュールを有し、前記設定されるセキュリティアソシエーションは前記加入者識別モジュールに格納されることを特徴とする請求項１記載のインターネットプロトコルセキュリティ実行方法。

【請求項８】　前記セキュリティアソシエーションの有効期間は長く、前記第一ノードと前記第二ノードとの間で行われる複数の通信セッションに渡って用いられることを特徴とする請求項１記載のインターネットプロトコルセキュリティ実行方法。

【請求項９】　前記通信はリアルタイム双方向デジタルデータ通信であることを特徴とする請求項１記載のインターネットプロトコルセキュリティ実行方法。

2

【請求項１０】　前記リアルタイム双方向デジタルデータ通信はインターネットプロトコルを用いた音声通信であることを特徴とする請求項９記載のインターネットプロトコルセキュリティ実行方法。

【請求項１１】　前記ネットワークは、国際移動通信規格２０００に適合したものであることを特徴とする請求項１記載のインターネットプロトコルセキュリティ実行方法。

【請求項１２】　移動ＩＰネットワークにおいて、ケルベロスを用いたインターネットセキュリティプロトコルを実行する方法であって、

ノードが無線基地局と無線による接続をしているときに、前記ノードと前期無線基地局との間で第二層の秘密鍵を設定する過程と、

前記設定された第二層の秘密鍵を前記ノード内において第二層から第三層へ通知する過程と、

前記ノードが前記ネットワークにログインするときに、前記ノードを前記ネットワークに認証させるために、前記通知された第二層の秘密鍵を用いる過程とを有することを特徴とするインターネットプロトコルセキュリティ実行方法。

【請求項１３】　前記ノードが行う通信はリアルタイム双方向デジタルデータ通信であることを特徴とする請求項１２記載のインターネットプロトコルセキュリティ実行方法。

【請求項１４】　前記リアルタイムデジタルデータ通信はインターネットプロトコルを用いた音声通信であることを特徴とする請求項１３記載のインターネットプロトコルセキュリティ実行方法。

【請求項１５】　前記ネットワークは国際移動通信規格２０００に適合したものであることを特徴とする請求項１２記載のインターネットプロトコルセキュリティ実行方法。

【請求項１６】　複数のノードがお互いにネットワークを介して通信を行い、

前記複数のノードのセキュリティアソシエーションを管理するための複数のセキュリティアソシエーション管理装置が前記ネットワーク上に設けられ、第二ノードとの通信を行う必要のある第一ノードから要求を受けると、一のセキュリティアソシエーション管理装置は、以前に前記第二ノードと行った通信の際に設定されたセキュリティアソシエーションが当該セキュリティアソシエーション管理装置内に格納されている場合は、当該セキュリティアソシエーションを前記第一ノードへ送信し、以前に前記第二ノードと行った通信の際に設定されたセキュリティアソシエーションが格納されていない場合は、当該セキュリティアソシエーション管理装置は当該セキュリティアソシエーションの設定を行い、設定されたセキ

ュリティアソシエーションを当該セキュリティアソシエーション管理装置内へ格納し、前記第一ノードへ送信することを特徴とするＩＰネットワーク。

【請求項１７】　前記ネットワークはケルベロス鍵交換法を採用し、通信を行う必要があるノードに対応したセキュリティアソシエーション管理装置に対し、セッション鍵を配布する鍵配布センタを備えることを特徴とする請求項１６記載のＩＰネットワーク。

【請求項１８】　前記セキュリティアソシエーション管理装置は、前記鍵配布センタに対しセッション鍵の発行を要求することを特徴とする請求項１７記載のＩＰネットワーク。

【請求項１９】　前記通信はリアルタイム双方向デジタルデータ通信であることを特徴とする請求項１６記載のＩＰネットワーク。

【請求項２０】　前記リアルタイム双方向デジタルデータ通信はインターネットプロトコルを用いた音声通信であることを特徴とする請求項１９記載のＩＰネットワーク。

【請求項２１】　前記ネットワークは国際移動通信規格２０００に適合するものであることを特徴とする請求項１６記載のＩＰネットワーク。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は広く無線通信ネットワーク及びモバイルインターネットプロトコルベースのネットワークにおいて導入されるインターネットプロトコルセキュリティ（ＩＰｓｅｃ）、特に「Ｖｏｉｃｅ ｏｖｅｒ ＩＰ」（ＶｏＩＰ）のような第三世代およびそれ以上の世代のリアルタイム・インタラクティブ・デジタルデータ通信、移動通信、インターネットプロトコルベースのデータ通信ネットワーク、または無線ＬＡＮに適用されるＩＰｓｅｃに関する。

【０００２】

【従来の技術】デジタルデータ通信ネットワークは、アメリカをはじめ、世界中で、ビジネス、商取引、あるいは一般の人々の生活においていたるところに顔を見せるようになった。公益的性格の強いインターネット、私的なプライベートローカルネットワーク（ＬＡＮ）、広域エリアネットワーク（ＷＡＮ）は、ますますデータ通信、データ送受信の重要なバックボーンとなっている。電子メール、ファイルアクセス、ファイル共有、サービスアクセスおよびサービス共有は、そのような多くのネットワークによって供給されるデータ通信サービスやデータ通信アプリケーションのうちのほんの一部でしかない。

【０００３】インターネットを含む今日のほとんどのデータ通信ネットワークは、実質的に同じアドレス管理プロトコルとルーティングプロトコルに従っている。このプロトコルにおいては、各々のネットワークにアクセス

することのできる装置（ノード）やネットワーク上に設けられたサーバ（ルータ）は、ＩＰアドレスと呼ばれるただ一つのアドレスを持っている。ネットワーク内またはネットワーク間でデジタルデータをやり取りするためには、送信者（送信ノード）はデータを「パケット」に分割して送信する。各々のパケットは送信ノードや所望の送信先ノードのＩＰアドレスやその他の情報のような、プロトコルによって定められている通信コントロールデータ、、、及び送信先ノードに送るべき実質的なデータを含んでいる。一回のデータの通信には、通信されるデータ量とその他の要素とに応じた数のパケットが作られ送信される。送信ノードは各々のパケットを別途独立に送信する。パケットはネットワーク上の中間ルータによって送信ノードから送信先ノードへと送られる。それら複数のパケットはかならずしも同じ経路をへて送信先ノードへ送られる必要はないし、また同時に到着する必要もない。なぜならパケット化の過程において各々のパケットには連続的な標識が付けられるからである。この標識によって送信先ノードは、たとえ異なった順番、異なる時間にパケットが届いたとしても、パケットを元の順番通りに再構成することができ、従ってパケットからもとのデータを再構築することができるのである。

【０００４】データ通信ネットワークの世界標準規格策定における認定機関であるインターネット学会の通信通信連合（ＩＴＵ）は、最近、国際移動通信規格（ＩＭＴ－２０００）を制定した。この規格は携帯電話、ＰＤＡ（Ｐｅｒｓｏｎａｌ Ｄｅｉｇｔａｌ Ａｓｓｉｓｔａｎｔｓ）、ハンドヘルドコンピュータ等の無線によって通信を行う広範囲な移動アクセスを考慮に入れた、いわゆる第三世代（３Ｇ）およびそれを超える世代（すなわち３．５Ｇ、４Ｇ等）のデータ通信ネットワークを提案している（ｈｔｔｐ：／／ｗｗｗ．ｉｔｕ．ｉｎｔ参照）。

【０００５】そのなかで提案されている第三世代およびそれをこえる世代の通信ネットワークは、データ通信に基づくＩＰをサポートしている。すなわち、すべてのネットワーク上のデータはデジタルデータであり、パケット単位で、そしてインターネットで用いられるアドレス管理プロトコル及びルーティングプロトコルに従ってやり取りされる。さらに、上述した第三世代及びそれ以上の世代無線通信ネットワークにおいては、移動ノードは、ネットワークに接続された他の固定ノードまたは移動ノードとデータ通信を行っている間、ネットワーク内を自由に移動することができる。従って、移動ノードがネットワーク接続やパケットの伝達経路を変更した場合、そのようなネットワークは、セキュリティや認証に関する問題を処理するとともに、移動ノードのアドレス管理装置、通信ノード間でやり取りされるデータパケットのダイナミックルーティングを提供しなくてはならない。

【０００６】近い将来、インターネットを使用するノードのうち大部分或いは少なくともかなりの部分を移動ノードが占めると予想されるので、この移動ノードに適合した通信ネットワークを構築することが特に重要となっている。インターネットアーキテクチャおよびインターネットの効率的利用に関すネットワークの設計者、運用者、ネットワーク機器の販売業者、学術研究者の国際的共同体であるインターネット技術特別対策委員会（ＩＥＴＦ）は、モビリティ支援に関するいくつかの規格を提案している（ｈｔｔｐ：／／ｗｗｗ．ｉｅｔｆ．ｏｒｇ参照）。これらの提案には、ＩＥＴＦのＲＦＣ２００２（モバイルＩＰバージョン４（ＩＰｖ４）とも呼ばれる）や「ＩＰｖ６におけるモバイル支援（Mobility Support in IPv6）」と表された草案「draft-ietf-mobileip-ipv6-13」（モバイルＩＰバージョン6とも呼ばれる）といったモビリティ支援に関する規格が含まれている。この２つの規格は本願明細書において参照として援用される。

【０００７】ＩＰｖ４やＩＰｖ６で定義されるプロトコル運用によると、移動ノードはその移動ノードのＩＰアドレスを変更せずにあるリンクから別のリンクへと移動することができる。ホームリンク上のホーム・サブネット・プレフィックス内で移動ノードに割り当てられた一個のＩＰアドレスである「ホームアドレス」によって移動ノードの位置は常に把握される。パケットはこのアドレスを用いて、移動ノードの現在どの地点からインターネットにアクセスしているかに関係なく転送され、移動体が別のリンクに移動しても、移動ノードは相手先ノード（固定ノード、移動ノードを含む）と通信を行い続けることができる。それゆえ、移動ノードがホームリンクから移動しても、トランスポート層と上位レイヤのプロトコルやアプリケーションに影響を与えない。

【０００８】モバイルＩＰｖ６はモバイルＩＰｖ４と多くの点で共通するが、プロトコルに関して言えば、完全にＩＰを包含しつつモバイルＩＰｖ４よりも多くの改良がなされている。例えば、「経路最適化」はモバイルＩＰｖ６のプロトコルの基本的な部分であるが、これはモバイルＩＰｖ４においては付加的な拡張オプションでしかなく、全てのノードでサポートされることは想定されていない。

【０００９】経路最適化機能によって移動ノードと相手先ノードとの間で直接的な経路が設定され、パケットの転送効率は最適化される。上述したように、それぞれの移動ノードは、現在のインターネットへの接続ポイントにかかわらず、常にホームアドレスによって識別される。移動ノードがホームリンクから離れている場合には、移動ノードは気付けアドレスとにも関連付けられており、そこには現在インターネットに接続している当該移動ノードの位置に関する情報が含まれている。

【００１０】モバイルＩＰｖ４においては、ホームから離れている使用されている移動ノードはホームエージェントに気付けアドレスを登録する。同様にモバイルＩＰｖ６においても、ホームリンクの外部に位置している移動ノードは、登録要求をホームエージェントに送信することによってホームエージェントに気付けアドレスを告知する。ホームエージェントは、登録要求を受信した後、当該移動ノード用宛のパケットを取得すると、当該移動ノードの気付けアドレスへトンネリングによって転送する。

【００１１】しかしながら逆方向の通信では、パケットは移動ノードから直接相手先ノードへ送られる。よって、いわゆるパケットのトライアングル・ルーティングが発生し、非対称パケット遅延の問題が生じてしまう。相手先ノードから移動ノードへの直接転送経路を確立するため、相手先ノードには、当該移動ノード現在の気付けアドレスを通知されるからである。モバイルＩＰｖ４においては、ホームエージェントが相手先ノードからホームから離れている移動ノード宛のパケットを受信したとき、バインディング情報をＩＰｖ４の移動ノードに送信することによって、直接転送経路が確立される。モバイルＩＰｖ６では、モバイルノードがバインディング更新を直接相手先ノードに対して送信することによって直接転送経路の確立がなされる。

【００１２】モバイルＩＰにおいてはセキュリティに関する問題も存在する。例えば、モバイルＩＰｖ４における位置登録プロトコルにおいては、移動ノードの通信は気付けアドレスにトンネリング転送されるホームエージェントとモバイルエージェントとの間で位置登録が認証されない場合、このトンネリング転送によって通信ネットワークは非常に脆弱なものとなってしまう可能性がある。さらに、モバイルＩＰｖ６においてバインディング更新は直接移動ノードへ転送されるのが標準となっている。従って、移動ノードと相手先ノードとの間でバインディング情報を含むパケットが認証されなかった場合、パケットの経路が変更されるとセキュリティ上の問題が生ずる可能性がある。モバイルＩＰを導入することによるこのようなセキュリティ上の問題は以前から指摘されていた。

【００１３】実際、関連ＲＦＣ提案においてそのようなセキュリティ上の問題が取り上げられているが、それらはモバイル環境においてＩＰセキュリティ（ＩＰｓｅｃ）導入の必要性を指摘するにとどまり、その具体的な導入方法には一切触れていない。ＩＥＴＦのモバイルＩＰ審議会においてはモバイル環境に適用可能なＩＰｓｅｃの構想に関して議論・研究されているにもかかわらずである。

【００１４】一方、ＩＰｓｅｃの構成の基礎はＩＥＴＦのＲＦＣ２４０１に「インターネットプロトコルのセキュリティ構成（Security Architecture for the Internet Protocol）」と称して規定されており、本願明細書

において参考として援用される。ＲＦＣ２４０１には、例えば接続の安定性、データ元の認証、秘匿性等の問題を扱うためのセキュリティサービスを含む、暗号を用いたＩＰｓｅｃが提案されている。基本的には、ＲＦＣ２４０１で提案されているＩＰｓｅｃは共通暗号鍵のみに依存しており、送信者と受信者の間の通信はその鍵によって暗号化、復号化される。したがって、ＲＦＣ２４０１で提案されるＩＰｓｅｃが機能するためには、送信者と受信者との間で安全な通信が行われる前に、暗号鍵と認証アルゴリズムまたは暗号化アルゴリズムと、そのアルゴリズムを実行するのに必要なパラメータとに関して両者の間で合意が成立している必要がある。この合意はセキュリティアソシエーション（ＳＡ）と呼ばれている。暗号鍵を設定する一般的な方法は鍵の配送・生成である。鍵の配送の例としては、第三者の認証機関から供給された共通な暗号鍵を利用する方法がある。鍵の生成方法で最も利用されているものの一つとして、ディフィ・ヘルマン（Diffie-Hellman；Ｄ－Ｈ）アルゴリズムがある。

【００１５】D-Hアルゴリズムは、送信者と受信者の各々は自分の持つ秘密の情報と相手の持つ公開情報とを数学的に結合させ共有の暗号値を計算する方法である。鍵管理プロトコルの詳細についてはＲＦＣの「インターネット・セキュリティ委員会および鍵管理プロトコル（Internet Security Association and Key Management Protocol）」を参考のため本願明細書において援用することとする。

【００１６】上述したＩＰｓｅｃはモバイルＩＰｖ４環境およびモバイルＩＰｖ６環境の両方に適用可能である。例えば、モバイルＩＰｖ４における、ホームから離れている移動ノードが気付けアドレスをホームエージェントに登録している間、当該ホームエージェントと当該移動ノードは互いに合意できるＳＡについて協議し、その後のトンネルを介した通信を保護するために用いられる暗号鍵を設定する。同様に、上記ＩＰｓｅｃはモバイルＩＰｖ６における経路最適化過程において実行される。すなわち、ホームから離れている移動ノードはバインディング更新を相手先ノードへ送信することによって、当該移動ノードの現在のインターネットへの接続ポイントを通知する。次に移動ノードと相手先ノードは互いに合意できるＳＡを協議し、その後の直接経路で行われる通信を保護するために使用すべき暗号鍵を決定する。

【００１７】上述した提案されているＩＰｓｅｃ構成は、比較的モバイルＩＰ環境でよく機能する。また、このＩＰｓｅｃの改良および効果的な実行に努力が払われている。しかし、以下の問題が考えられる。例えば、モバイル環境において提案されているＩＰｓｅｃは、経路最適化がなされたときに移動ノードと相手先ノードとの間でＳＡを設定する過程において一定の時間が必要となる。ＩＰｓｅｃの本来の目的からすると、保護すべき通信はＳＡが確立される前に行われてはならない。従って、ＳＡの確立のためには時間が必要であり、これは明らかに通信の遅延を招く。通信の遅延は、電子メールやファイルの送受信に関しては深刻な問題を引き起こさないかもしれない。そのようなデータ通信はリアルタイムの双方向アプリケーションでなく、したがって特に通信の遅延には影響されないからである。

【００１８】

【発明が解決しようとする課題】しかしながら、近年のＶｏＩＰやリアルタイム双方向マルチメディアのようなリアルタイム双方向データ通信の登場により、モバイル環境においてＩＰｓｅｃを導入することはかなり困難になってしまっている。電子メールやファイルの送受信と違い、リアルタイムデータ通信アプリケーションはタイミングのずれに非常に敏感である。特にＶｏＩＰはイントラネットワーク処理、送受信、ルーティング遅延に非常に敏感である。ＳＡの確立に要する時間に起因した通信の遅延は、鍵を設定する際にＤ－Ｈアルゴリズムのような大量の計算を必要とする鍵生成方法が用いられた場合に、より顕著となる。

【００１９】

【課題を解決するための手段】本発明の目的は必要な認証およびセキュリティアソシエーション設定過程で生ずるパケット遅延を減少させる方法を提供することである。具体的には、本発明は、受信ノードがパケットを送信ノードから受信した後その過程を初期化するのを待つのではなく、当該送信ノードがユーザ認証およびセキュリティアソシエーションの設定を初期化することができる方法を提供する。

【００２０】本発明の方法によれば、送信ノードは受信ノードとの間の通信を初期化し、当該受信ノードに対してセキュリティアソシエーションが設定されたかどうかを判定する。当該セキュリティアソシエーションが設定されていない場合、送信ノードはセキュリティアソシエーションの設定を初期化する。受信ノードが自分のホームリンクの外部にいることもあるが、この場合には当該受信ノードは送信ノードからパケットを受信した後バインディング更新を送信する。本発明においては、送信ノードがバインディング情報を受信ノードから受信する前にセキュリティアソシエーションの設定が初期化される。従って、本発明の方法をもちいることによって、認証とセキュリティアソシエーションの設定の過程において発生するパケット遅延が減少する。

【００２１】本発明の一態様においては、認証およびセキュリティ確保の過程においてケルベロス鍵交換方法が用いられる。ケルベロス鍵交換方法は計算量が少なくて済むので、ＰＤＡや携帯電話等のあまりリソース利用ができない機器が主に利用する通信ネットワークであるモバイルＩＰ通信ネットワークに適している。計算量が少

ないため認証およびセキュリティアソシエーションの確立に要する時間は少なくて済む。よって、認証及びセキュリティアソシエーションに起因するパケット遅延はさらに減少する。

【００２２】本発明の別の態様において、モバイルノードの無線通信ネットワーク制御装置（ＲＮＣ）に対するレイヤ２の秘密鍵は、レイヤ３の事前共有秘密鍵としても用いられ、当該移動ノードが当該通信ネットワークにアクセスする際の認証がなされる。これによって、移動ノードにおいて鍵の管理作業が用意になる。

【００２３】本発明のさらに別の態様において、通信ネットワークは当該通信ネットワークに接続されるノードのＳＡを管理するＳＡ管理装置を備えている。ＳＡ管理装置を設けることによって、ＰＤＡや携帯電話等のリソースの少ないノードの消費メモリ量およびノードが行うべき計算量が軽減される。携帯電話の消費メモリ量は、加入者識別モジュール（ＳＩＭ）にＳＡを格納しておくことによっても削減可能である。

【００２４】

【発明の実施の形態】本発明の好適な実施形態を図面を参照しつつ説明する。この図面において、同様の構成要素には同一の参照符号が付される。本願明細書における好適な実施形態の説明は本質的な意味において例示に過ぎず、本発明の範囲を限定するものではない。

【００２５】図１に本発明が適用される第三世代の無線モバイルアクセスＩＰネットワーク１００の一例を示す。データ通信ネットワーク１００は、モバイルアクセス通信ネットワークに対するＩＭＴ―２０００規格およびＩＴＵの仕様に従うものとする。加えて、データ通信ネットワーク１００は、ＩＥＴＦで提案されているモバイルＩＰｖ６およびモバイルＩＰｖ４標準規格に従い、モバイルＩＰ支援を実行する。これらの規格および仕様はＩＴＵおよびＩＴＥＦのウェブサイトで公開されており、本願明細書において参照として援用される。

【００２６】無線モバイルアクセスＩＰ通信ネットワーク１００の中心には、多数の図示せぬノードつまり固定の接続ポイントまたはリンクを有する固定ノードＩＰデータ通信ネットワーク１２０が設けられている。インターネットプロトコルバージョン６などのインターネットプロトコルに従って、デジタルデータは通信ネットワーク内または通信ネットワークを介してやり取りされる。インターネットプロトコルバージョン６はＩＴＥＦのＲＦＣ２４６０に規定されており、これを本願明細書において参照として援用することとする。基幹通信ネットワーク１２０には複数の関門ルータ１３０が設けられており、これらが集まってＩＰモバイルバックボーン１４０を形成している。データパケットは、従来のインターネットアドレス管理およびルーティングプロトコルに従い、ネットワークに接続された送信元から送り先ノードへと転送される。おのおのの関門ルータ１３０は一つのＩＰアドレスを持ち、ホームエージェント（ＨＡ）またはフォーリンエージェント（ＦＡ）として機能するサーバ又はルータ１４５と接続されており、移動ノード１３５および相手先ノード１４０とコア・ネットワーク１２０とを接続している。これはＩＴＥＦのＲＦＣ２００２（「Ｍｏｂｉｌｅ　ＩＰ　Ｖｅｒｓｉｏｎ４」）で規定されているもので、これは本願明細書において参照として援用される。移動ノードと及び相手先ノードは異なる種類の携帯受話器、携帯電話機、ハンドヘルドコンピュータ、ＰＤＡ（Ｐｅｒｓｏｎａｌ　Ｄｉｇｉｔａｌ　Ａｓｓｉｓｔａｎｔｓ）、無線データ通信端末等のモバイル無線通信デバイスであってもよい。

【００２７】ＲＦＣ２００２に従うと、移動ノード１３５及び相手先ノード１４０は一つのホームネットワークが与えられる。各ノード１３５，１４０は、そのホームネットワーク上での実質的なルータであるホームエージェント１４５をさらに有する。おのおのの移動ノード１３０および相手先ノード１４５が自身のホームネットワーク内に位置しているときは、そのホームエージェントが通信ネットワーク１２０への接続ポイントとなる。すなわち、移動ノードがホームネットワーク内にいる場合は、当該移動ノードのホームエージェント１４５は移動ノードからのパケットを転送する。

【００２８】また、提案されているモバイルＩＰ支援の規格に従うと、モバイルノードのホームエージェント１４５は、移動ノード１３５の現在位置に関する情報、すなわち当該移動ノードの気付けアドレスを保持し、移動ノード１３５がそのホームネットワークエリアから離れて作動しているとき、少なくとも提案されている基本的なモバイルＩＰｖ４規格では、パケットの転送およびトンネリング送信をホームネットワークエリアの外部に位置している当該移動ノード１３５に対して行い続ける。

【００２９】他のルータ１４５はフォーリンエージェントとして機能する。フォーリンエージェントは、移動ノードがホームネットワークエリアの外部で動作するときは、当該移動ノード１３５に対しアクセスポイントを提供する。移動ノードが、ある時間および位置において接続している通信ネットワークに属するフォーリンエージェントは、当該移動ノード１３５から、また当該移動ノード１３５へとパケットを転送する機能を有する。各エージェント１４５は無線基地局通信ネットワーク１５０を有しており、モバイルノード１３５および１４０と通信を行うようになっている。各無線基地局通信ネットワーク１５０は複数の無線基地局（ＢＴＳ）を有している。移動ノード１３５および１４０、ＢＴＳはＣＤＭＡ、Ｗ―ＣＤＭＡまたは同様なデジタルデータ通信技術を用いて、相互に通信を行う。ＢＴＳ通信ネットワーク１５０および１５５の構成、配置および機能は従来の一般的なものである。同様に、無線移動ノード１３５およびＢＴＳ１５５にはＣＤＭＡ，Ｗ―ＣＤＭＡや同様のデ

ジタルデータ通信技術が標準的に用いられる。その詳細な説明は、本発明の理解には必要でない故省略する。

【００３０】各ノードは開放型システム間相互接続（ＯＳＩ）規格に準拠しパケットの送受信を行う。ＯＳＩ規格は７つの離散的レイヤ、すなわちアプリケーション層（第７層）、プレゼンテーション層（第６層）、セッション層（第５層）、トランスポート層（第４層）、ネットワーク層（第３層）、データリンク層（ＭＡＣ）（第２層）、および物理層（第１層）における通信プロトコルの実行の枠組みを定義している。ＯＳＩ規格によれば、送信ノードの第７層から始まり、制御は一つの層から次の層へ渡されてゆき、第一層まで下っていく。そして通信ネットワークを介して、相手先ノードにおいて、制御が最下層から最上位層まで上っていく。最下層では基本的な通信プロトコルの制御が行われる。例えば、第一層はＢＴＳへビットデータを送信したり、ＢＴＳから受信したりする。この層はビットのもつ意味を解釈しないが、信号の電気的特性および物理的な特性あるいは信号方式を取り扱う。第２層はＢＴＳとの通信における伝送データのビット誤りおよびビット列フォーマットを担当する。すなわちこの層はビットの意味をある程度解釈し、ＢＴＳとの間の通信プロトコルを取り扱う。第３層はネットワーク上の通信経路の確立を担当する。この層は、データの意味を完全に解釈しアドレス管理（アドレッシング）、ルーティングおよびセキュリティプロトコルの処理を行う。

【００３１】データ通信ネットワーク１００全体において、移動ノードモビリティには３つの段階がある。第一に、マクロモビリティとは、移動ノードがホームネットワークから他のエージェントが属する通信ネットワークに移って位置が変化するような場合である。換言すれば、移動ノードのデータ通信ネットワークへのリンクあるいは接続があるエージェントから別のエージェントへと移る場合である。マクロモビリティはホームエージェントとフォーリンエージェントとの間、あるいはフォーリンエージェント間の変化であり、エージェント間モビリティとも呼ばれる。第二に、中間モビリティとは、移動ノードがそのリンクをあるＢＴＳの属する通信ネットワークから、別のＢＴＳの属する通信ネットワークへ移す際の、移動ノードの位置変化のことを言う。最後にマイクロモビリティとは、通信ネットワークリンクが変化せずにＢＴＳ通信ネットワーク１５０内の移動ノードの位置が変化する場合のことをいう。

【００３２】無線移動通信ネットワークにおける中間モビリティとマイクロモビリティの取り扱い方とは良く知られている。例えば、良く知られている方法に、ビーコン信号強度を用い、移動ノード装置１３５がマクロモビリティスケールでその位置を変えたとき、ＢＴＳ間における通信ハンドオフを行うものがある。あるいは、移動ノード１３５がＢＴＳ通信ネットワークの境界をまたいで位置を変更したとき、ＢＴＳ間の通信ハンドオフが行われるのも標準的な方法である。どちらの方法をとるにせよ、その詳細な説明は本発明を理解するのに特に必要ではないのでここでは省略する。

【００３３】移動ノードが通信ネットワーク内において、通信ネットワークリンクをあるエージェントから別のエージェントに変更するようなマクロモビリティレベルに関して本発明が適用される。図２はモバイルＩＰｖ６を適用した、第三世代の無線移動アクセスデータ通信ネットワークにおける移動ノードのマクロモビリティとハンドオフ過程を示す簡略図である。この例において、移動ノードのマクロモビリティに起因するエージェント間の通信ネットワーク接続ハンドオフ処理は、提案されているモバイルＩＰｖ４についてはＩＴＥＦのＲＦＣ２００２に、提案されているＩＰｖ６については「www.ietf.org./internet-drafts」のなかの「draft-ietf-mobileip-ipv6-12.txt」にそれぞれ規定されている。

【００３４】図２において通信ネットワーク１００はＩＰｖ６ネットワーク１２０およびＩＰｖ６ネットワーク１２０に接続されるルータすなわちエージェント１４５で構成される。ハンドオフ過程は移動ノード（ＭＮ）１３５が初めに位置Ａにいるときに開始されるとする。図に示す例では、ＭＮ１３５はホームリンク内で動作しており、ホームエージェント１４５を介してネットワーク１２０と接続されている。ＭＮ１３５は、好ましくはホームエージェントＨＡ１４５を含むエージェント１４５と無線により、ＣＤＭＡ、Ｗ－ＣＤＭＡまたは同様な無線広帯域スペクトル拡散信号技術等を用いて、図示せぬＢＴＳと通信を行う。

【００３５】モバイルＩＰｖ６およびモバイルＩＰｖ４規格は、モビリティ検知およびハンドオフの機能を提供する。どちらのバージョンにおいても、ＭＮ１３５のモビリティは近隣探索（Neighbor Discovery）メカニズムによって検知され、移動ノードが最初のエージェントのカバーするエリアから２番目のエージェントがカバーするエリアへ入ったとき、最初のエージェントから二番目のエージェントへの移動ノードのネットワーク接続のハンドオフが行われることになる。従って、この例ではモバイルＩＰｖ６通信ネットワークに関して図示しているが、モバイルＩＰｖ４に関しても同様な機能および要件が存在する。

【００３６】ＭＮ１３５が初期位置Ａから中間地点である位置Ｂへ移動すると、その動きはＩＰ移動検出方法または好ましい方法の組み合わせによって検出される。モバイルＩＰｖ６における主な検出方法は、ＩＰｖ６のルータ発見（Router Discovery）や近隣到達不能検出（Neighbor Unreachability Detection）を含む、ＩＰｖ６の近隣探索を実行する設備を用いるものである。ＩＴＥＦのＲＦＣ２４６１の「ＩＰバージョン６のための近隣探索（Neighbor Discovery for IP version 6(IPv

6))」に詳細に記載されており、本願明細書において参照のため援用される。これはＩＰｖ６の移動ノードに対し、すでに言及し本願明細書において援用されているＩＴＥＦのモバイルＩＰバージョン６の草案において推奨されているものである。

【００３７】位置Ａから位置Ｂを経由して位置Ｃへと移動する間、ＭＮはルータ発見を使って新しいエージェントおよびリンクが張られているサブネットプレフィックスを探す。ルータ発見処理は、ＭＮによるルータ要請メッセージのブロードキャストを含む。フォーリンエージェント１４５（ＦＡ１）がルータ要請メッセージを受信できるくらい十分にＭＮの近傍にいるときは、当該フォーリンエージェントは直接ＭＮ１３５に対しルータ通知メッセージを送信することになる。あるいは、ＭＮ１３５は単にＦＡ１からの非請求（定期的）ルータ通知を待っているだけでも良い。ＭＮ１３５がＦＡ１からルータ通知メッセージを受信すると、ＭＮは自己のデフォルトルータリストおよび、自己のプレフィックスリスト内のＦＡ１のサブネットプレフィックスのエントリを保持する。このようにして、デフォルトルータリストによって、当該ＭＮ１３５が新しい通信ネットワーク接続を確立できるＭＮデフォルトエージェントの候補のひとつとしてＦＡ１は特定されるのである。

【００３８】ＭＮ１３５がＨＡ１４５から離れている間は、ＭＮは、新しいエージェントと新しい気付けアドレスとに切り替える為に、ＨＡと送受信不可能になった時点をすばやく検知できるかどうかが重要である。デフォルトエージェントと送受信不可能になった時点を検知するために、ＭＮ１３５は隣接到達検知を用いる。図２において、ＭＮ１３５が中間地点Ｂに到達し位置Ｃ方向へ移動しつつあるとき、ＨＡを介して行われていたネットワーク接続状態は劣化する。通信状態の劣化は、ＭＡＣ層（第２層）によって検出されるＬ２ビーコン信号強度の減少および通信エラーの増大という形で現れる。ＨＡ１４５から到達可能かどうかは、（１）ＭＮ１３５がＨＡ１４５と通信しているならば、パケットに対するＨＡ１４５からの応答として受信するＴＣＰ応答確認の損失があるかどうか、または（２）ＨＡ１４５からの非請求マルチキャストルータ通知メッセージの損失があるかどうか、または（３）明示的近隣通知メッセージに対する応答としてＨＡ１４５からの近隣通知メッセージが受信されないかどうかによって決定される。ＭＮ１３５がＨＡ１４５との通信状態の劣化を検出し始めたら、ＭＮ１３５はハンドオフ処理を開始し完全にＨＡ１４５と通信不能になってしまうまでの間にその処理を完了しなくてはならない。ＭＮ１３５はまず、デフォルトルータリストを検索しＦＡ１を探す。次に当該ＦＡ１との通信リンクを確立し、ＨＡ１４５との通信リンクを切断する。

【００３９】ＨＡ１４５とＦＡ１との間の通信ハンドオフ処理にあたって、Ｍｎ１３５は新たなフォーリンエージェントを特定するための気付けＩＰアドレスを取得する必要がある。自動アドレス設定の好ましい方法としては、ＩＴＥＦ　ＲＦＣ２４６２の、「ＩＰｖ６　ステートレスアドレス自動設定」に規定されており、本願明細書ではこれを援用する。この方法によれば移動ノードの新たな気付けアドレスは、ＦＡ１から通知されるサブネットプレフィックスリスト内のＦＡ１のサブネットプレフィックスから生成される。ハンドオフ処理が終了した後、ＭＮ１３５が位置Ｃに到達する時間までには、フォーリンエージェントＦＡ１を介してネットワークリンクが確立されることとなる。

【００４０】図３は新たな気付けアドレスの登録の過程およびハンドオフ処理が完了した後の経路最適化の過程を要約した図である。ステップ１において、ＭＮ１３５はＨＡ１４５からフォーリンエージェント（ＦＡ１）へとネットワーク接続のハンドオフを行う。次にＭＮ１３５は、ＦＡ１から送信されるＦＡ１のサブネットプレフィックスにより生成される気付けアドレスを設定し（ステップ２）、バインディング更新をＦＡ１を介してＨＡへと送信する。ＨＡ１４５は当該バインディング更新を受け取ると、該気付けアドレスをＭＮ１３５用のバインディングキャッシュに登録することによって、ＭＮのホームアドレスと現在の気付けアドレスとの関連付けがなされる。バインディングキャッシュにおける関連付けにはある有効期間が設定されており、それを経過するとその関連付けは無効となる。

【００４１】ＭＮ１３５がネットワーク接続をＦＡ１へとハンドオフした後、相手先ノード（ＣＮ）１４０が該ＭＮ１３５と通信を開始する必要になったとする。さらに、該ＣＮ１４０は一度も該ＭＮ１３５と通信を行ったことがなく、該ＭＮの変わることのないホームアドレスを除き、該ＭＮの現在位置に関する情報を持っていない。従って、該ＣＮは第一パケットを該ＭＮのホームネットワークへ送信する（ステップ３）。ＨＡ１４５は、該ＣＮ１４０から送信されたパケットを取得し、該ＭＮの現在の気付けアドレス用のバインディングキャッシュを検索する。次に、ＨＡ１４５はこのパケットをカプセル化したのち、新たなパケットを生成し、これを該ＦＡ１を介して現在のＭＮの気付けアドレスをあて先として該ＭＮ１３５へトンネル送信する。

【００４２】「 HYPERLINK "http://www.ietf.org/internet-drafts" www.ietf.org/internet-drafts」に掲載されている「draft-ietf-mobileip-optim-09.txt」において規定されている、提案中の拡張モバイルＩＰｖ４規格では、ＭＮ１３５とＣＮ１４０との間で直接通信経路を確立することによって、パケットルーティングの最適化が図られている。この提案中の拡張規格の本質的な部分は、既述したようにモバイルＩＰｖ６規格にすでに組み込まれている。ＭＮ１３５は、ＨＡ１４５からカプセル化されトンネル送信されたパケットを受信すると、該

Hアルゴリズムを置き換えるものである。ケルベロスは他のセキュリティ保護がされていないネットワークに対し、既共有秘密鍵に基づいて秘密鍵暗号化アルゴリズムを用いた認証サービスを提供する。ＩＴＥＦ１５１０の「ケルベロスネットワーク認証サービス（The Kerberos Network Authentication Service (V5)）」に詳細な記載があり、これを本明細書において参照のため援用することとする。

【００４９】前述した規格で提案されるＩＰｓｅｃは、その実行および鍵管理の対応する準備ができているにもかかわらず、ケルベロスを用いる事に関しては何も言及していない。実際、ケルベロス等の方法は当該提案されているＩＰｓｅｃの枠組みにはうまく適合しない。ＲＦＣ２４０１において定義されている、ＩＰｓｅｃの集中鍵管理を作成するための標準化過程プロトコルを取り決めるために結成されたワーキンググループは、現在、ＲＦＣ１５１０で定義されているケルベロスアーキテクチャを用いてＩＰｓｅｃ用の暗号化音声プロトコル作成中である。

【００５０】ケルベロスは従来の暗号化技術すなわち、信頼できる第３者の認証サービス機関から配布される共有秘密鍵を用いて認証を行う。図４は、ケルベロス鍵交換方法を用いたユーザ認証確立までの処理とＳＡの設定とを簡単にまとめた図である。ノードａおよびノードｂは信頼できる第３者認証サービス機関である同一の鍵配布センタ（ＫＤＣ）の管轄であり、各ノードはそれぞれ既登録の秘密鍵Ｋａおよびを ＫｂをＫＤＣに保有している。たとえば、ノードａとノードｂとがある小一つのネットワークに接続しているとき、これらの秘密鍵はＫＤＣに登録される。したがって、ノードａとＫＤＣは秘密鍵Ｋａを共有し、ノードｂとＫＤＣは秘密鍵Ｋｂを共有していることになる。秘密鍵ＫａおよびＫｂは通常半永久的に変わらないものと考えてよい。

【００５１】ここで、ノードａがノードｂと通信を行うにあたって、ＫＤＣに対して、ノードａとノードｂ間の通信の暗号化・復号化に必要なセッション鍵の発行を依頼するとする（ステップ１）。この依頼に対し、ＫＤＣはセッション鍵Ｓａｂを準備するとともに、秘密鍵Ｋｂを用いてセッション鍵Ｓａｂを暗号化した鍵を準備する。このセッション鍵Ｓａｂは、特にノードａとノードｂ間での通信のセッションを暗号化・復号化するのに用いられ、従って秘密鍵ＫａおよびＫｂとは異なり、短い有効期間しか持たない。次にＫＤＣは秘密鍵Ｋａを用いて、セッション鍵Ｓａｂおよび秘密鍵Ｋｂで暗号化されたセッション鍵Ｓａｂの両方を暗号化しノードａへ送信する（ステップ２）。ノードａは復秘密鍵Ｋａを用いて、受け取ったセッション鍵Ｓａｂと、秘密鍵Ｋｂで暗号化されたセッション鍵Ｓａｂ（第２の鍵）とを復元する。第二の鍵は秘密鍵Ｋｂによって暗号化されているため、ノードａはこれ以上この鍵を復号化することができない。ステップ３ではノードａはこの第二の鍵をノードｂへ送信する。ノードｂは秘密鍵Ｋｂを用いてこの第二鍵を復号化しセッション鍵Ｓａｂを復元する。このようにノードａおよびノードｂはセッション鍵Ｓａｂを共有することで、当該ノード間における以降の通信において、通信の暗号化および復号化がなされる。ノードｂが秘密鍵Ｋｂを用いて第二の鍵を復号化できるということは第二の鍵がＫＤＣで発行されたものであるということである。なぜなら、ＫＤＣとノードｂだけが秘密鍵Ｋｂを知っているからである。また、各ノードａおよびｂは以降の通信をセッション鍵Ｓａｂを用いて復号化することができるということは、送信者の認証ができるということでもある。なぜなら、ＫＤＣ、ノードａ、ノードｂだけがセッション鍵Ｓａｂを知っているからである。

【００５２】図５から図７を用いて本発明の好適な方法の詳細を説明する。図５から図７は本発明のＩＰｓｅｃを実行する方法を示したフローチャートである。これらの図におけるデータ通信ネットワークは図３におけるものと同一である。すなわち、第三世代若しくはそれを超える世代の無線移動アクセスインターネットプロトコルベースのデータ通信ネットワークあるいは無線ＬＡＮである。したがって、図中のネットワークはＩ、Ｐｖ４規格とＩＰｖ６規格とに適合し、モバイルＩＰｖ４およびＩＰｖ６の両方をサポートする。当該ネットワークはＩＭＴ－２０００規格にも適合し、ＣＤＭＡ、Ｗ－ＣＤＭＡまたはその他の無線広帯域スペクトル拡散信号処理技術を用いた無線による移動アクセスをサポートする。図に示す態様においては、ＶｏＩＰにようなリアルタイム双方向マルチメディアデータ通信がネットワーク内で行われる。また、図に示されている処理はＭＮ１３５がＨＡ１４５からハンドオフを完了し、当該ＭＮの気付けアドレスがＨＡ１４５に登録されたときに始まるものである。さらに、図中のＫＤＣは二つのサーバとしての機能を有する。すなわち、認証サーバ（ＡＳ）とチケット交付サーバ（ＴＧＳ）である。ＡＳはＴＧＳに対するノードの認証を行う。ＴＧＳは、お互いに通信を望んでいるノードに対しセッション鍵およびチケットの発行を行う。

【００５３】図５において相手先ノード（ＣＮ）１４０はＭＮと通信を開始しようとしている。ＣＮ１４０のバインディングキャッシュは当該ＭＮの現在の気付けアドレスはまだ更新されていないとする。ＣＮは当該ＭＮと通信を行うために、まずＣＮは当該ＭＮに対して第一パケットを当該ＭＮのホームネットワークへ送信する（ステップ１）。第一パケットは制御パケットであり、その中身は実行すべきアプリケーションによるが、一例を挙げれば、ＶｏＩＰにおける単なる接続要求である。第一パケットは常に保護すべきデータを含んでいるとは限らないので、ＩＰｓｅｃの保護なしで送信されてもかまわないと考えられる。この第一パケットはＨＡによって受

MNのホームアドレスと該MNの現在の気付けアドレスが関連付けているバインディング情報を該ＣＮ１４０が持っていないことを認識する。ステップ４において、該ＭＮ１３５はバインディング更新を該ＣＮ１４０に送信する。該ＣＮ１４０はバインディング更新を受信すると、バインディングキャッシュに該MNの恒久的なホームアドレスと関連づけて格納されている該MNの気付けアドレスのエントリを保持する。この後、該ＣＮ１４０から送信される該ＭＮ１３５宛の全てのパケットは、該ＣＮ１４０から該ＭＮ１３５へ直接伝送される。従って、このような経路最適化をおこなうことにより、いわゆるトライアングル・ルーティングに起因するパケット遅延の問題は解消される。

【００４３】上述したバインディング処理において、該ＭＮ１３５の正当性を担保するため、および盗聴、能動的リプレイ攻撃、その他の攻撃、秘密データへの不正アクセス等の問題を回避するため、該ＭＮ１３５と該ＣＮ１４０間において、認証およびセキュリティアソシエーションも行われる。特に、もしバインディング更新を送信しているＭＮ１３５がＣＮ１４０において正しく認証されていない場合、あるいは、以降の通信に必要な正しいセキュリティアソシエーションがＭＮ１３５とＣＮ１４０間で確立されていない場合、この経路最適化機能は深刻なセキュリティ上の問題を引き起こす可能性がある。本願明細書においてすでに援用されているＩＴＥＦのモバイルＩＰｖ６の草案にはこれらのセキュリティ上の問題が指摘されている。

【００４４】ＩＴＥＦのＲＦＣ２４０１の「Security Architecture for the Internet Protocol」（本願明細書においてすでに援用済み）において、ＩＰｖ４およびＩＰｖ６の両方について、暗号ベースのＩＰセキュリティ（ＩＰｓｅｃ）の基本的なアーキテクチャが提案されている。ＩＰｓｅｃは認証および秘匿性（暗号化）を含むセキュリティ上のサービス群を提供する。ＲＦＣ２４０１にしたがえば、ＩＰｓｅｃはふたつのセキュリティプロトコル、すなわち認証ヘッダ（ＡＨ）と暗号ペイロード（ＥＳＰ）、および暗号鍵管理の手続きおよびプロトコルを用いて実行される。ＡＨとＥＳＰはＩＰｓｅｃを実行する上において重要な役割をする。その詳細はＲＦＣ２４０２の「IP Authentication Header」およびＲＦＣ２４０６の「IP Encapsulating Security Payload」に記載されており、参照のため本願明細書において援用する。暗号鍵管理手続きおよびプロトコルについては、ＲＦＣ２４０８の「Internet Security Association and Key Management Protocol (ISAKMP)」に記載があり、これは本願明細書にすでに援用済みである。

【００４５】ＲＦＣ２４０１で提案されているセキュリティ方式およびプロトコルのなかで、セキュリティアソシエーション（ＳＡ）はＩＰｓｅｃの実行の際に最も基本となるものである。ＳＡは二つのノード間の関係であり、お互いのノードが安全に通信を行うことを目的として、使用することを合意しているセキュリティサービスを記述するものである。ＳＡはセキュリティパラメータインデックス（ＳＰＩ）とＩＰ送り先アドレスとセキュリティプロトコル（ＡＨまたはＥＳＰ）識別子との３つによって一意に決定される。ＳＰＩはセキュリティプロトコルの識別子である。ＩＰ送り先アドレスは、通信相手ノードのホームアドレスまたは気付けアドレスを示している。各々のノードは、現在通信中のノードまたはすでに通信したことのあるノードの各々に対し、一つのＳＡを持っている。各ＳＡには予め決められた時間が経過すると無効になるような有効期間が設定されている。ノード間で保護されるべきデータを含んだパケットがやり取りされる前にＳＡが設定されなければならない。

【００４６】ＳＡの設定は、ＲＦＣ２４０１で提案されているような暗号ベースのＩＰｓｅｃにおける鍵管理プロトコルの重要な部分である。暗号ベースのＩＰｓｅｃの背景にある基本的な考え方は、通信の暗号化および複合化の際に使われる秘密セッション鍵を二つのノードが共有するという点にある。よって、ＳＡを設定する際には必ず秘密セッション鍵の設定が必要になる。鍵の設定には二つの方法がある。一つは鍵輸送とよばれ、信頼できる第三者機関である鍵配布センタ（ＫＤＣ）が、ネットワークドメイン内にある全てのノードの秘密セッション鍵を保有し、通信を開始したいノードに対して秘密セッション鍵を配布するというものである。もう一つは鍵生成と呼ばれる方法である。この鍵生成の例として、秘密セッション鍵を生成するためにディフィ・ヘルマン（Diffie-Hellman ；Ｄ－Ｈ）アルゴリズムを用いるものがある。Ｄ－Ｈアルゴリズムは二人のユーザが公開鍵を交換することから始まる。各ユーザは他のユーザの情報を自分の情報とを数学的に結合させ秘密の値を算出するのである。この秘密の値は、セッション鍵としてまたはランダムに生成されるセッション鍵を暗号化する際に必要となる鍵として用いられる。

【００４７】ユーザ認証およびＳＡの設定を実行するのにかなり時間がかかり、パケット遅延をもたらすことは当業者にとって明らかである。本発明はユーザ認証およびＳＡの設定によるパケット遅延の問題の解決を図ることを目的としている。本発明は、相手先ノードは、移動ノードが第一パケットを相手先ノードから受信した後ユーザ認証およびＳＡセキュリティの設定を初期化するのを待つのではなく、自ら初期化処理を実行することができるような方法を提供する。

【００４８】さらに、本発明は、移動ノードと相手先ノード間で伝送されるデータの暗号化・復号化を行う際に一般的に用いられているが多大な量の計算を必要するため深刻なパケット遅延を招きかねない従来のＤ－Ｈ公開鍵アルゴリズムに取って代わるものである。本発明は、比較的計算の負荷が少ないケルベロス鍵交換方法でＤ－

信されＨＡから当該ＭＮへトンネル送信される（ステップ２）。ＣＮで実行すべきアプリケーションにも依存するが、この第一パケットは制御パケットでなくても良く、当該ＭＮに送信される前にＩＰｓｅｃによって保護されたデータであっても良い。そのような場合、ステップ１および２は省略され、すぐにステップ３に移り、当該ＣＮと当該ＭＮ間でセキュリティアソシエーション（ＳＡ）が設定される。

【００５４】図５におけるネットワークの全ての構成要素は、ＩＰｓｅｃを実行するための第一の手段としてケルベロスを用いることに同意している。従って、ネットワークは一つの鍵配布センタ（ＫＤＣ）を備え、ここで当該ネットワークで用いられる全ての暗号鍵を管理している。上述したようにＫＤＣは認証サーバ（ＡＳ）およびチケット交付サーバ（ＴＧＳ）で構成される。さらに、ＭＮとＫＤＣは、当該ＭＮが当該ネットワークにログインした時点で発行された秘密鍵Ｋｍｎを共有している。ＣＮおよびＫＤＣは同様にＣＮがネットワークにログインした時点で発行された秘密鍵Ｋｃｎを共有している。購入時に秘密鍵を作り、ＫＤＣと秘密鍵を共有し、ネットワークにアクセスするための機器にはいろいろな種類がある。

【００５５】第一パケット送出した後、ＣＮはセキュリティアソシエーション（ＳＡ）キャッシュを参照し、当該ＭＮとの間で設定済みのＳＡがあるかどうかをチェックする（ステップ３）。図８は本実施形態で用いられるＳＡキャッシュを示す。図において、ＳＡキャッシュには複数のＳＡエントリがある。ひとつのＳＡエントリは、当該ＣＮが現在通信しているかまたは過去に通信したことがあるひとつのノードに対応している。ＳＡは、セキュリティパラメータインデックス、セキュリティプロトコル識別子およびＩＰ送信先アドレスを含むいくつかのパラメータによって特定される。この３つのパラメータについてはすでに説明したのでここでは省略する。この３つのパラメータに加えて、本実施形態におけるＳＡはさらに二つのパラメータを有する。一つは「ＩＰ送信先ホームアドレス」と呼ばれるもので、もうひとつは「第一パケットフラグ」と呼ばれるものである。ＩＰ送信先ホームアドレスには、通信相手のノードのホームアドレスが格納されている。第一パケットフラグは、第一パケットが、ＳＡが設定されていない状態でノードに送信されたときにオンとなり、他方ＳＡが設定されたときオフとなる。ＳＡには有効期間があり、ある時間が経過すると無効になる。すなわち、有効期間が経過するとＳＡエントリは当該ＳＡキャッシュから消去される。

【００５６】図５ステップ３において、ＣＮは自身のＳＡキャッシュを検索し、当該ＭＮに対するＳＡエントリがあるかどうかを確かめる。ＭＮに対するＳＡキャッシュがある場合、ＣＮはステップ４の処理に進み以降のパケットは、ＳＡキャッシュに格納されているセキュリティパラメータインデックスによって特定されるケルベロスセッション鍵を用いて暗号化され、当該ＭＮへ送信される。該当するＳＡエントリが存在しない場合、ＣＮはステップ５の処理に進む。ＣＮが当該ＭＮと一度も通信を行ったことがない場合、当該ＭＮに対するＳＡエントリは存在しない。

【００５７】さらに、ＣＮがＭＮと以前通信を行ったことはあるが、それがかなり昔である場合、当該ＭＮに対するＳＡエントリは無効になっており、ＳＡキャッシュからも消去されている。当該ＭＮに対するＳＡエントリが見つからなかった場合、以降のＭＮとの通信を保護するために、新たなＳＡを設定する必要がある。従来のＩＰｓｅｃプロトコルにおいては、このような場合、バインディング更新をＭＮから受信した時点でＣＮはＳＡの設定を開始していた。具体的には、ＭＮがＣＮからの送信されＨＡによってトンネル送信された第一パケットを受信すると、該ＭＮはＣＮが現在のＭＮの位置を知らないということを認識し、当該ＣＮに対してバインディング更新を送信し、当該ＣＮは自身のバインディングキャッシュを更新するのである。ＣＮがＭＮから送信されたバインディング更新を受信した後、ＳＡが設定される。換言すれば、従来のＩＰｓｅｃにおいては、ＭＮはＣＮへバインディング更新を送信することによってＳＡを初期化するのである。しかしながら、ＳＡがＭＮとＣＮとの間で設定されるまで、実質的に両者の間で通信を行うことはできない。よって、従来のＩＰｓｅｃを用いたＳＡの設定においてはバインディング更新がＣＮに届くまでＳＡの設定を開始することができないために重大なパケット遅延をもたらすということは当業者にとって容易に分かることである。

【００５８】本発明においては、ＣＮは、ＭＮがＣＮからの第一パケットを受信した後ＳＡ設定の初期化するのを待つのではなく、ＣＮがＳＡ設定の初期化を行うことができる。ステップ５においてＣＮは、図８に示す自身のＳＡキャッシュ内に当該ＭＮに対するＳＡエントリを１つ指定し第一パケットフラグをオンにする。第一パケットフラグがオンであるということは、すなわちＳＡの設定が現在行われているということを意味する。セキュリティ保護されるべきパケットデータはＳＡが設定されるまで送信することができないが、制御パケットは保護されていない状態で送信することができる。

【００５９】ＣＮは以降の制御パケットをＭＮに対して送信することは許されるが、第一パケットフラグによって、ＭＮとの間でのＳＡの設定を繰り返し初期化することは禁止される。次に、ＣＮはＫＤＣと通信を行うことが許可されているかどうかを判断する。具体的には、ＣＮは自身をＫＤＣに認証してもらうためのケルベロスチケットを自身が持っているかどうかを判断する。持っていない場合、最初の認証処理（ステップ６）へ進み、ＫＤＣからチケットを取得する。すでに持っていた場合

は、ステップ７へと進み、ＫＤＣに対して、当該ＭＮと通信を行えるようにするため、認証サービスを要求する。

【００６０】ステップ６の詳細を図６に示す。最初の認証ステップ（ステップ６）において、ユーザはまずユーザ名を入力するよう求められる（ステップ６－１）。続いて、ＣＮはケルベロス認証要求（ＫＲＢ＿ＡＳ＿ＲＥＱ）を該ユーザ名とともにＡＳへ送信する（ステップ６－２）。ユーザ名の確認および秘密鍵Ｋｃｎの抽出後、ＡＳはセッション鍵ＳｃｎおよびチケットＴｃｎを生成する（ステップ６-３）。ＡＳはセッション鍵ＳｃｎおよびチケットＴｃｎを、秘密鍵Ｋｃｎを用いて暗号化したうえで、これをケルベロス認証応答（ＫＲＢ＿ＡＳ＿ＲＥＰ）としてＣＮへ送信する。Ｋｃｎ｛Ｓｃｎ、Ｔｃｎ｝はセッション鍵とチケットＴＣｎとの両方が秘密鍵Ｋｃｎで暗号化されたことを意味する。ＣＮはＫＲＢ＿ＡＳ＿ＲＥＰを受信すると、秘密鍵Ｋｃｎで復号化しセッション鍵ＳｃｎおよびチケットＴｃｎを復元する（ステップ６－５）。ＣＮは自身をＴＧＳに対して認証してもらうためのチケットＴｃｎを取得したので、ステップ７へ進む。ステップ７の詳細を図７に示す。

【００６１】図７においてＣＮはＴＧＳに対し、チケットＴＣｃｎとともに、ＭＮと通信するためのセッション鍵の発行を要求を送信する（ステップ７－１）。チケットＴｃｎはＴＧＳに自身を認証させるための証明書の役割を持つ。チケットＴｃｎの認証が完了した後（ステップ７-２）ＫＤＣはステップ３においてセッション鍵Ｓｃｎ/ｍｎ、セッション鍵ＳｍｎおよびチケットＴｍｎを生成する。セッション鍵ＳｍｎはＭＮとＫＤＣ間の通信を保護するために利用され、チケットＴｍｎはＭＮをＫＤＣに認証させるための証明書として用いられる。ＭＮはＫＤＣと通信を行い、セッション鍵ＳｍｎおよびチケットＴｍｎがすでに設定されている場合、ＴＧＳはこの鍵およびチケットを発行することはない。

【００６２】まず、セッション鍵Ｓｃｎ/ｍｎ、セッション鍵ＳｍｎおよびチケットＴｍｎが秘密鍵Ｋｍｎを用いて暗号化される（Ｋｍｎ｛Ｓｃｎ/ｍｎ，Ｔｍｎ，Ｓｍｎ｝）。次にＴＧＳはセッション鍵Ｓｃｎ／ｍｎとＫｍｎ｛Ｓｃｎ／ｍｎ、Ｔｍｎ，Ｓｍｎ｝の両方を秘密鍵Ｋｃｎを用いて暗号化（Ｋｃｎ｛Ｓｃｎ／ｍｎ、Ｋｍｎ｛Ｓｃｎ／ｍｎ，Ｔｍｎ，Ｓｍｎ｝｝）し、ＣＮへ送信する（ステップ７－４）。ステップ７-５においてＣＮは秘密鍵Ｋｃｎを用いてこれらの鍵を復号化しセッション鍵Ｓｃｎ／ｍｎおよびＫｍｎ｛Ｓｃｎ／ｍｎ，Ｔｍｎ，Ｓｍｎ｝を取り出す。Ｋｍｎ｛Ｓｃｎ／ｍｎ，Ｔｍｎ，Ｓｍｎ｝は秘密鍵Ｋｍｎによって暗号化されているのでＣＮはこれ以上復号化することはできない。次にＣＮはＫｍｎ｛Ｓｃｎ／ｍｎ，Ｔｍｎ，Ｓｍｎ｝を送信するがこれらはＨＡによって受信され、ＭＮへトンネル送信される（ステップ７－６）。ＭＮはＫｍｎ｛Ｓｃｎ／ｍｎ，Ｔｍｎ，Ｓｍｎ｝を受信するとこれを秘密鍵Ｋｍｎを用いて復号化しセッション鍵Ｓｃｎ／ｍｎ、Ｔｍｎ，Ｓｍｎを取り出す（ステップ７－７）。

【００６３】図５に戻りステップ７の処理が完了すると、ＣＮは自身のＳＡキャッシュに格納されている、当該ＭＮと通信を行うために設定されたＳＡのエントリを保持する（ステップ８）。具体的には図８に示すＳＡキャッシュにおいて、ＣＮは、セッション鍵Ｓｃｎ／ｍｎを特定するためのセキュリティパラメータインデックスを含む必要な情報を当該ＭＮに対するＳＡエントリに格納する。ＣＮはさらに、同一のエントリの第一パケットフラグをオフにする。対応するＳＡエントリはＭＮのＳＡキャッシュ内にも生成される。

【００６４】ＣＮおよびＭＮは同一のセッション鍵Ｓｃｎ／ｍｎを共有するので以後安全に通信を行うことができる。最後に、ＭＮは、ＣＮから送信された第一パケットの応答として、バインディング更新をＣＮに送信する（ステップ９）。本発明の方法を用いれば、ＣＮがＳＡ設定を初期化することができるのでＳＡ設定に起因するパケット遅延が劇的に減少する。

【００６５】図９は本発明の別の実施形態を示したものである。本実施形態において、上記のＣＮが移動ノードの場合、移動ノードと無線通信ネットワーク制御装置（ＲＮＣ）との間における第二層における認証用の秘密鍵が第三層における認証用の鍵としても用いられる。ＲＮＣは呼制御、接続制御、無線インターフェースサポートおよびモビリティ管理のような第二層通信プロトコルを実装している。移動ノードがネットワークに対して初めて無線接続を試みるとき、ＲＮＣに対して当該移動ノードを認証させるための第二層の秘密鍵が生成される。

【００６６】他方、上記秘密鍵ＫｍｎおよびＫｃｎはＫＤＣとの間で生成され、第三層での認証の際に使用される。換言すれば、移動ノードからネットワークに対し無線による接続が確立されたとき、当該移動ノードは第二層での認証用の秘密鍵を持っていなければならない。接続が確立した後、当該移動ノードは自身をＫＤＣに認証させるために、別の、第三層における認証用の秘密鍵を持っている必要がある。確かに二つの鍵の使用目的は異なるが、二つの別途独立した秘密鍵を生成することは煩雑でかつ無駄であるということは当業者にとって明らかである。従って、本実施形態においては、このような無駄を省くため第二層の秘密鍵が第三層の秘密鍵としても利用できるようになっている。

【００６７】図９に一つの秘密鍵が第二層と第三層の両方の認証に対して用いられる無線データ通信ネットワークを示す。同図においてＣＮは移動ノードであり、無線接続が確立したとき、自身とＲＮＣとの間の通信で用いる第二層の秘密鍵を生成する（ステップ１）。第二層の秘密鍵がＲＮＣから当該通信ネットワーク上にあるＫＤＣに送信される。ＣＮの内部では、第二層の秘密鍵は第

三層へ通知される。従ってＣＮおよびＫＤＣは同一の秘密鍵を共有することとなる。ＣＮをＫＤＣに認証させるために、ＣＮとＫＤＣ間における第三層の秘密鍵を生成する必要はない。ＣＮがＭＮと通信をする必要がある場合には、ＣＮは上述したように、ＳＡ設定を初期化しＫＤＣに対して、ＣＮと当該ＭＮ間で通信を行うためのセッション鍵の発行を要求する（ステップ３）。

【００６８】ＣＮはセッション鍵の発行要求を受信すると、ＫＤＣと共有している当該ＣＮの第二層の秘密鍵を用いて、自身をＫＤＣに認証させる。次にＫＤＣは、セッション鍵およびＭＮの第二層の秘密鍵で暗号化したセッション鍵をＣＮへ送信する。ついで、この二つの鍵は自身の秘密鍵によって復号化される（ステップ４）。次に当該ＣＮは、まだＭＮの第二層の秘密鍵によって暗号化されている当該セッション鍵をＭＮへ送信し（ステップ５）、ＭＮの秘密鍵によってこのセッション鍵は復号化される。

【００６９】図１０は本発明の更に別の態様を示したものである。セッション鍵は通信のセッションを保護するために発行され、ある有効期限を持つ。したがって、新たな通信セッションが始まるときは新たなセッション鍵をＫＤＣから取得しなければならない。また、予期せぬ通信上の問題のため、通信セッションが完了するのに時間がかかってしまう場合、セッション鍵はセッションの途中で無効になってしまう可能性もある。

【００７０】仮にセッション鍵がセッションの途中で無効になったとすると、当該通信セッションは中止せざるを得ず、新たなセッション鍵をＫＤＣから取得するまでは通信を再開することができない。図１０に示すネットワークにおいて、セッション鍵の有効期間は長く、複数の通信セッションに渡って再使用すること可能である。しかしながら、セッション鍵の有効期間を長くするとノードは多くのＳＡエントリを持っていなければならなくなる可能性がある。通常、移動ノードは、多くのＳＡエントリを格納しておけるだけの十分なメモリ空間を有していない。この問題を解決するために、図１０におけるネットワークは、当該ネットワークに接続される移動ノードに代わってＳＡを管理するＳＡ管理装置を備えている。

【００７１】図１０において、ＣＮがＭＮと通信を行う必要が生じたとき、当該ＣＮは上述したようにＳＡ設定を初期化しセッション鍵の発行を自己のＳＡ管理装置Ａに要求する（ステップ１）。当該ＳＡ管理装置Ａは、この要求に対する応答として、当該ＣＮと当該ＭＮ間の通信を保護するためのＳＡの設定に対するＳＡエントリを検索する。ＳＡの有効期間は長いので、当該ＣＮと当該ＭＮと以前に通信を行ったことがある場合、ＣＮとＭＮとの間での以前に行われた通信に対して設定されたＳＡがまだ残っている可能性がある。

【００７２】ＳＡ管理装置Ａがまだ以前の通信に対するＳＡを保存している場合、当該ＳＡ管理装置はＳＡによって特定されるセッション鍵を当該ＣＮへ送信する。ついで当該ＣＮは、以前に当該ＭＮと通信で使われたこのセッション鍵で暗号化したパケットを当該ＭＮへ送信する。当該ＭＮは当該ＣＮよりこのパケットを受信すると、自己のＳＡ管理装置Ｂに対してＣＮから受信したパケットを復号化するためのセッション鍵の発行を要求する。セッション鍵の以前の通信からの有効期間は、ＳＡ管理装置Ａと（Ｂ）で同一である。従って、同一のセッションはＳＡ管理装置Ｂでもいまだ有効であるはずである。ＳＡ管理装置Ｂは要求の応答として、セッション鍵を当該ＭＮへ送信する。当該ＭＮはＳＡ管理装置Ｂから受け取ったセッション鍵を用いてＣＮから受信したパケットを復号化する。

【００７３】ＳＡ管理装置ＡがＣＮとＭＮの間の通信に関するＳＡを持っていない場合は、ＳＡ管理装置ＡはＫＤＣに対し、新たなセッション鍵の発行を要求する（ステップ２）。これに対しＫＤＣはセッション鍵を当該ＳＡ管理装置Ａへ送信する（ステップ３）。ＳＡ管理装置ＡはＭＮとの通信を行うためのＳＡを内部で生成し、当該セッション鍵をＣＮとＳＡ管理装置Ｂとへ送信する（ステップ４）。次に、ＳＡ管理装置Ｂは対応するＳＡを設定し、当該セッション鍵ＭＮへ送信する（ステップ５）。

【００７４】上述したように、当該セッション鍵は、ＣＮの秘密鍵とＭＮの秘密鍵とによって保護された状態で、ＫＤＣとＣＮ間およびＣＮとＭＮ間で配布される。ＳＡの有効期限は長い（したがってセッション鍵のそれも長くなる）ため、ＫＤＣに鍵の発行を要求する頻度は少なくてすむ。しかるに、ＫＤＣがセッション鍵を発行することに起因するパケット遅延も減少する。また、伝送されるパケットの数に基づいて通信コストは算出される。ＫＤＣに対するセッション鍵の発行要求の回数が少なくなるので、ＳＡを設定するために必要なパケットの数も減少し、通信コストの削減になる。

【００７５】図１１は本発明の更に別の実施形態を適用した無線データ通信ネットワークを示す図である。図１０に示した実施形態と同様、ＳＡおよびセッション鍵の有効期間は長い。しかしながら、図１１に示す本実施形態においては、ＳＡは携帯電話内の購入者識別モジュール（ＳＩＭ）に格納される。ＳＩＭはマイクロチップが組み込まれたスマートカードである。

【００７６】マイクロチップには、購入者のアカウントの詳細がサービスへのアクセス情報および設定情報とともに格納されている。本実施形態で導入されるＩＰｓｅｃプロトコルは図１０に示す実施形態のそれと同様である。すなわち、ＣＮはＭＮと通信を行う必要になったとき、当該ＣＮは携帯電話ＰｃｎのＳＩＭに格納された、当該ＣＮと当該ＭＮ間での通信を保護するために設定されたＳＡのＳＡエントリを参照する。

【００７７】携帯電話機ＰｃｎのＳＩＭが以前の通信で設定されたＳＡをまだ保有している場合は、当該ＳＩＭはそのＳＡで特定されるセッション鍵をＣＮに通知する。ＣＮは以前に行われた通信で用いられたセッション鍵を用いて暗号化されたパケットをＭＮへ送信する。ＭＮはＣＮから暗号化されたパケットを受信すると、携帯電話機ＰｍｎのＳＩＭに格納されたセッション鍵を取得し、当該携帯電話機ＰｍｎのＳＩＭから取得したセッション鍵を用いて、ＣＮから受信したパケットを復号化する。

【００７８】ＣＮとＭＮ間での通信のＳＡが携帯電話機ＰｃｎのＳＩＭに格納されていない場合は、ＣＮはＫＤＣに対して新しいセッション鍵の発行を要求する（ステップ１）。これを受けてＫＤＣは当該ＣＮにセッション鍵を送信する（ステップ２）。ＣＮはＭＮとの通信用のＳＡを生成し、携帯電話機ＰｃｎのＳＩＭに格納する。次にＣＮはこのセッション鍵をＭＮへ送信する（ステップ３）。そしてＭＮは対応するＳＡを生成し、携帯電話機ＰｍｎのＳＩＭに格納する。

【００７９】上述したように、セッション鍵はＣＮの秘密鍵とＭＮの秘密鍵とによって保護された状態で、ＫＤＣとＣＮ間およびＣＮとＭＮ間での配布される。図１０に示す実施形態と同様に、本実施形態においても、ＳＡおよびセッション鍵の有効期間が長いので、ＫＤＣに対してセッション鍵の発行の要求頻度は少ない。したがって、ＫＤＣのセッション鍵の発行に起因するパケット遅延は減少する。ＫＤＣに対してセッション鍵の発行要求の頻度が少ないということはＳＡを設定するために必要なパケット数も少なくて済み、通信コストの削減になるということである。加えて、本実施形態においては、図１０に示されるような、通信に介在するＳＡ管理サーバ等の中間サーバは必要ではないので、通信の安全性は増す。

【００８０】ここまで本発明の好適な実施形態について説明してきたが、各実施形態は単なる例示であり本発明の本質を限定するものではない。また、本発明の趣旨を逸脱しない範囲において、本発明の新規および優位な特徴を保ったままで、本発明に対し種々の変形あるいは付加を施すことは、当業者にとって容易に理解される。したがって、本発明の範囲は正しく解釈された請求の範囲のみに基づいて定まるものである。

【００８１】

【発明の効果】以上説明したように、本発明の方法によれば、必要な認証およびセキュリティアソシエーション設定過程で生ずるパケット遅延が減少する。

【図面の簡単な説明】

【図１】　本発明が実施される第三世代の無線モバイルアクセスＩＰ通信ネットワークの模式図である。

【図２】　モバイルＩＰを用いた第三世代の無線モバイルアクセスＩＰ通信ネットワークにおけるモバイルノードを示すマクロモビリティを示す簡略図である。

【図３】　モバイルＩＰを用いた第三世代の無線モバイルアクセスＩＰ通信ネットワークにおけるモバイルモビリティと経路最適化の結果を示す簡略図である。

【図４】　ケルベロス鍵交換方法の実行ステップを示す簡略図である。

【図５】　本発明のＩＰｓｅｃを実行過程を示すフローチャートである。

【図６】　本発明における最初の認証過程と鍵発行過程とを示すフローチャートである。

【図７】　本発明における共有鍵の設定の過程を示すフローチャートである。

【図８】　本発明において用いられるセキュリティアソシエーションの模式図である。

【図９】　レイヤ２の秘密鍵がレイヤ３の秘密鍵としても用いられる、本発明の第２実施形態を実行するモバイルＩＰ通信ネットワークの簡略図である。

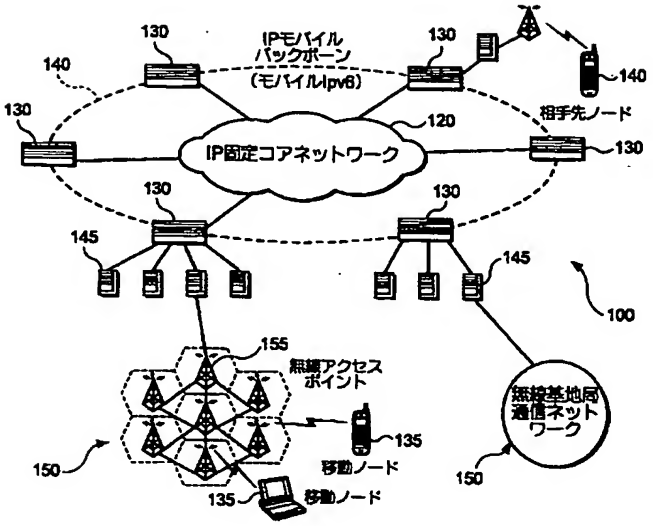
【図１０】　ノードのセキュリティアソシエーションを管理するセキュリティアソシエーション管理装置を用いた、本発明の第三実施形態を実行するモバイルＩＰ通信ネットワークの簡略図である。

【図１１】　セキュリティアソシエーションが携帯電話機の加入者識別モジュール格納される、本発明の第４実施形態を実行するモバイルＩＰ通信ネットワークの簡略図である。

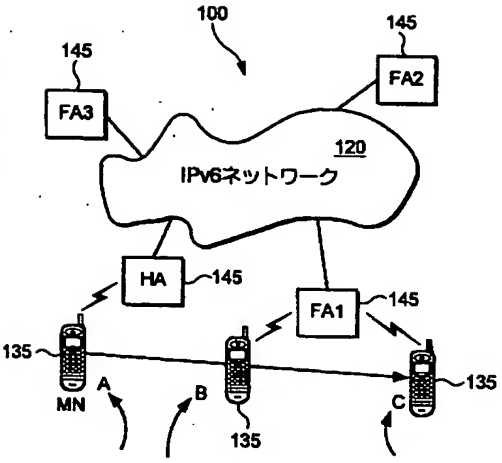
【符号の説明】

１００　移動ＩＰネットワーク
ＦＡ　フォーリンエージェント
ＨＡ　ホームエージェント
ＭＮ　移動ノード
ＣＮ　相手先ノード
ＫＤＣ　鍵配布センタ
ＲＮＣ　無線通信ネットワーク制御装置

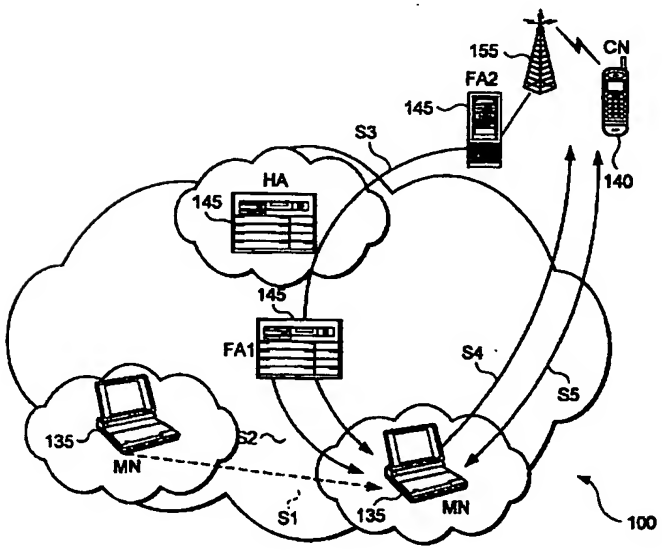
【図１】


130
IPモバイル
バックボーン
(モバイルIpv6)
130
140
140
相手先ノード
130
120
IP固定コアネットワーク
130
130
145
145
145
100
155
無線アクセス
ポイント
135
移動ノード
150
135
移動ノード
150
無線基地局
通信ネット
ワーク

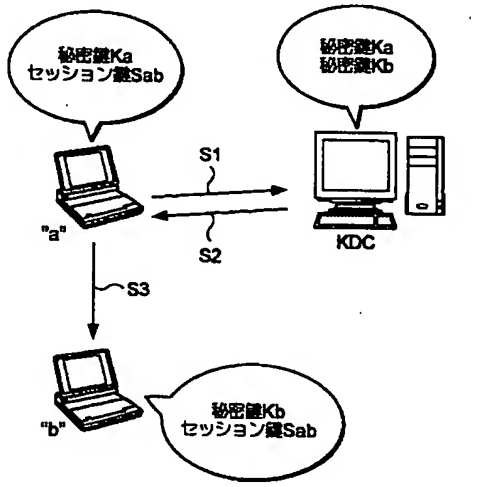
【図２】


100
145
145
FA2
FA3
120
IPv6ネットワーク
HA
145
FA1
145
135
MN
A
B
135
C
135

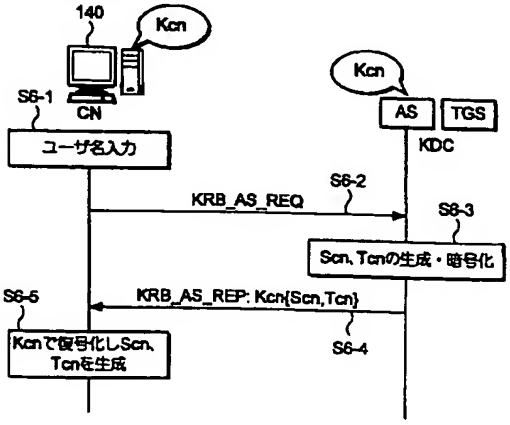
【図３】


155
CN
FA2
145
S3
140
HA
145
145
FA1
S4
S5
135
MN
S2
S1
135
MN
100

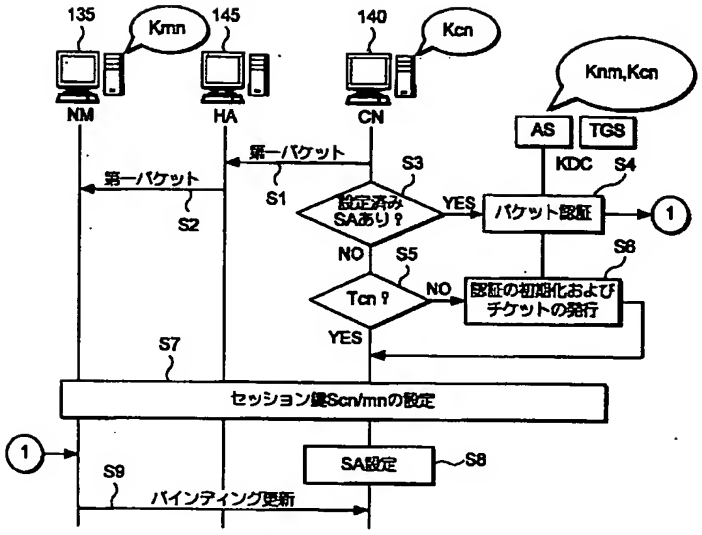
【図４】


秘密鍵Ka
セッション鍵Sab
秘密鍵Ka
秘密鍵Kb
S1
"a"
S2
KDC
S3
"b"
秘密鍵Kb
セッション鍵Sab

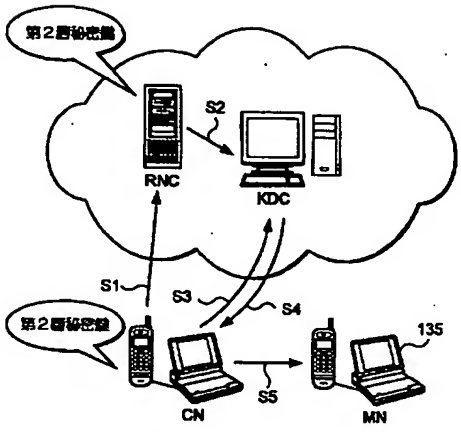
【図６】


140
Kcn
Kcn
S6-1
CN
AS
TGS
KDC
ユーザ名入力
S6-2
KRB_AS_REQ
S6-3
Scn, Tcnの生成・暗号化
S6-5
KRB_AS_REP: Kcn{Scn,Tcn}
S6-4
Kcnで復号化しScn、
Tcnを生成

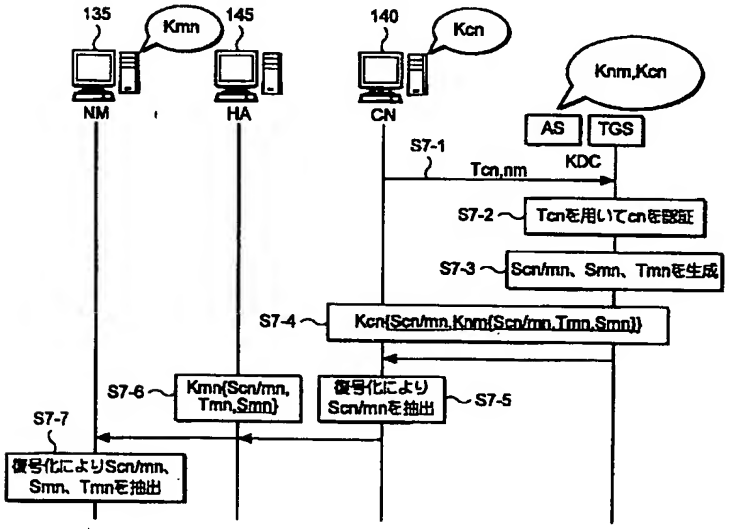
【図５】



【図９】



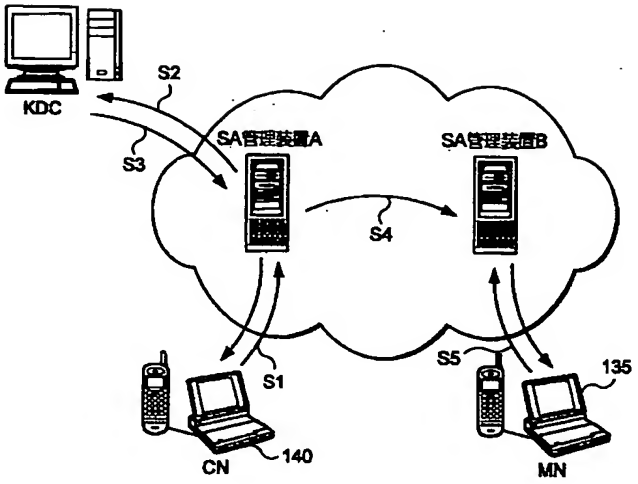
【図７】



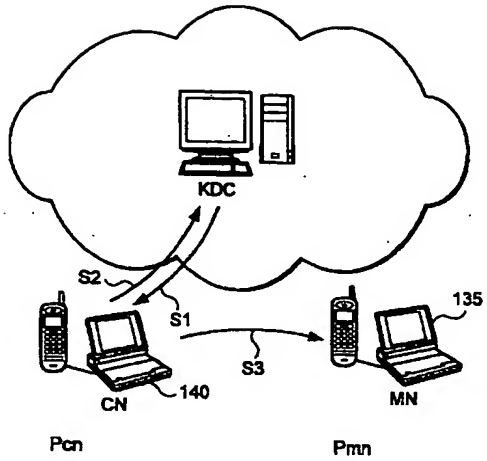
【図８】

セキュリティパラメータインデックス	セキュリティプロトコル識別子	IP送り先アドレス	・・・	IP送り先ホームアドレス	第一パケットフラグ

【図１０】



【図１１】



フロントページの続き

(72)発明者　ヨコテ　アキ
アメリカ合衆国，カリフォルニア州
95110，サンノゼ，スイート300，メトロ
ドライブ181

Ｆターム(参考)　5J104 PA07
5K030 GA15 HA08 HC09 JT09 LD19
5K067 AA30 AA32 BB21 DD17 EE02
EE10 EE16 HH21 HH36

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☑ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☑ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.